IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Jerry Chow	§	Art Unit:	2432
		§		
Serial No.:	10/813,003	§	Confirmation No.:	5213
		§		
Filed:	March 31, 2004	§	Examiner:	Jung W. Kim
		§		
For:	Memory Protection Systems and Methods for Writable Memory	§ § §	Atty. Dkt. No.:	NRT.0199US (15923ROUS04U)

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF PURSUANT TO 37 C.F.R § 41.37

Sir:

The final rejection of claims 1-17, 19, 20, 22-28, 30, 32, 34-36, 39, 41 and 43-47 is hereby appealed.

I. REAL PARTY IN INTEREST

The real party in interest is Nortel Networks Limited.

II. RELATED APPEALS AND INTERFERENCES

None.

III. STATUS OF THE CLAIMS

Claims 1-17, 19, 20, 22-28, 30, 32, 34-36, 39, 41 and 43-47 have been finally rejected and are the subject of this appeal. Claims 18, 21, 29, 31, 33, 37-38, 40, and 42 have been cancelled.

IV. STATUS OF AMENDMENTS

No amendment after the final rejection of May 20, 2009 has been submitted. Therefore, all amendments have been entered.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

Independent claim 1 recites a memory protection system comprising:

a key store (Fig. 1:18) to store identifiers of protected memory locations and respective corresponding memory protection keys (Spec., p. 8, ln. 4-18; p. 11, ln. 4-17); and

a memory access manager (Fig. 1:16) including at least hardware (Spec., p. 9, ln. 6-7) configured to:

receive (Fig. 3:32) a memory command for altering contents of any of the protected memory locations (Spec., p.19, ln. 3-6; p. 19, ln. 26 – p. 20, ln. 2),

determine (Fig. 3:36) whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered, wherein the memory protection key in the memory command is written to a volatile memory (Spec., p.20, ln. 10-17),

if the memory command includes the memory protection key corresponding to each protected memory location to be altered, permit (Fig. 3:40, 42) the memory command to proceed (Spec., p.21, ln. 5-11), and

then render (Fig. 4:44) the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile storage such that the memory protection key written to the volatile memory is inaccessible after completion of the memory command (Spec., p.21, ln. 8-11; p. 17, ln. 13-18).

Independent claim 16 recites an electronic device comprising:

a memory (Fig. 1:20; Spec., p. 8, ln. 1-4);

a wireless receiver (Fig. 1:12) configured to receive data relating to a remote software update to be written to the memory (Spec., p. 6, ln. 13-15; p. 14, ln. 11-18);

a memory protection system (Fig. 1:16, 18) associating protected memory locations in the memory with respective corresponding keys, and configured to allow the received data to be written to any of the protected memory locations only if the received data includes a key corresponding to the protected memory location to which the received data is to be written and to render the corresponding key in the received data inaccessible after allowing the received data to be written to the protected memory location (Spec., p. 8, ln. 1-18; p. 11, ln. 4-17, 28-29; p. 14, ln. 4-10; p. 21, ln. 5-11); and

volatile storage (Fig. 1:22) having unprotected memory locations, the memory protection system configured to download the received data including the key to the unprotected memory locations of the volatile storage prior to writing the received data to the protected memory locations, and the memory protection system to render the key inaccessible by overwriting at least a portion of the key (Spec., p. 5, ln. 20; p. 17, ln. 13-18; p. 20, ln. 3-9).

Independent claim 22 recites a method of protecting memory (Fig. 1:20; Spec., p. 8, ln. 1-4) in an electronic device, comprising:

receiving (Fig. 3:32) a memory command to access a protected memory location (Spec., p. 19, ln. 6-8; p. 19, ln. 26 – p. 20, ln. 2);

determining whether the received memory command is a memory read command to read the protected memory location, or a memory write command to alter the protected memory location (Spec., p. 19, ln. 8-16);

in response to determining that the received memory command is the memory write command (Spec., p. 19, ln. 10-13):

identifying (Fig. 3:36) a memory protection key corresponding to the protected memory location (Spec., p. 20, ln. 10-17);

determining (Fig. 3:36)whether the memory write command includes the memory protection key corresponding to the protected memory location, wherein at least the memory protection key in the memory write command has been written to volatile memory (Spec., p. 20, ln. 10-17);

permitting (Fig. 3:40, 42) completion of the memory write command if the memory write command includes the memory protection key corresponding to the protected memory location (Spec., p. 21, ln. 5-11); and

rendering (Fig. 4:44) the memory protection key in the memory write command that has been written to the volatile memory inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory inaccessible after completion of the memory write command (Spec., p. 21, ln. 8-11; p. 17, ln. 13-18); and

in response to determining that the received memory command is the memory read command, processing the memory read command to read the protected memory location without checking for any memory protection key (Spec., p. 19, ln. 13-15).

Independent claim 36 recites a method of protecting electronic memory (Fig. 1:20; Spec., p. 8. ln. 1-4), comprising:

configuring a memory store (Fig. 1:20, 18) of an electronic device into at least one protected memory location and a key store operable to store an identifier of each protected memory location and a respective corresponding memory protection key (Spec., p. 8, ln. 1-18; p. 11, ln. 4-17); and

configuring a processor (Fig. 1:14) of the electronic device to provide a memory access manager operable to receive memory commands for altering contents of any of the at least one protected memory location (Spec., p. 20, ln. 10-17), and for at least one memory command, to:

determine (Fig. 3:36) whether the at least one memory command includes a memory protection key corresponding to at least one protected memory location to be modified, said at least one memory command including the memory protection key corresponding to at least one said protected memory location to be modified (Spec., p. 20, ln. 10-17),

permit (Fig. 3:40, 42) the at least one memory command to complete (Spec., p. 21, ln. 5-11), and

then render (Fig. 3:44) each corresponding memory protection key in the at least one memory command inaccessible by overwriting at least a portion of the memory protection key upon completion of the at least one memory command, wherein the at least one memory command corresponds to a remote software update received by a wireless receiver for updating the at least one protected memory location to be modified (Spec., p. 21, ln. 8-11; p. 17, ln. 13-18; p. 19, ln. 26-29).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1, 9, 10, 22-28, 30, 32, 34, 35, 41 and 46 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bryant, US 5,628,023 in view of Bishop Computer Security, Chapter 29.5 "Common Security-Related Programming Problems"

B. Claims 1, 2, 4, 7-9, 11-15 and 46 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Beukema US Patent Application Publication No. 2002/0124148 in view of Bishop

C. Claims 16, 17, 19, 20, 22, 25, 36, 39, 43-45 and 47 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hind, US 6,976,163 in view of Bryant and Bishop

D. Claims 1 and 3-6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over England, US 7,194,092 in view of Bishop

VII. ARGUMENT

The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-headings as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Claims 1, 9, 10, 22-28, 30, 32, 34, 35, 41 and 46 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bryant, US 5,628,023 in view of Bishop Computer Security, Chapter 29.5 "Common Security-Related Programming Problems"

1. Claims 22-25, 30, 32, 34, 35.

Independent claim 22 was rejected as purportedly obvious over Bryant in view of Bishop.

Claim 22 recites a method of protecting memory in an electronic device, comprising:

- receiving a memory command to access a protected memory location;
- determining whether the received memory command is a memory read command to read the protected memory location, or a memory write command to alter the protected memory location;
- in response to determining that the received memory command is the memory write command:

- identifying a memory protection key corresponding to the protected memory location;
- determining whether the memory write command includes the memory protection key corresponding to the protected memory location, wherein at least the memory protection key in the memory write command has been written to volatile memory;
- permitting completion of the memory write command if the memory write command includes the memory protection key corresponding to the protected memory location; and
- rendering the memory protection key in the memory write command that has been written to the volatile memory inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory inaccessible after completion of the memory write command; and

- in response to determining that the received memory command is the memory read command, processing the memory read command to read the protected memory location without checking for any memory protection key.

As conceded by the Examiner, Bryant fails to disclose rendering the memory protection key in the memory write command inaccessible by overwriting at least a portion of the memory protection key upon completion of the memory write command. 5/20/2000 Office Action at 9-10. Instead, the Examiner cited Bishop as purportedly disclosing the claimed feature missing from Bryant. *Id.* at 10.

It is respectfully submitted that a person of ordinary skill in the art would not have been prompted to combine the teachings of Bryant and Bishop. As taught by Bryant, a user program stores a token in a register location. Bryant 19:41-42. Subsequently, when the user program issues an instruction to modify the information currently stored in a previously protected page, the user program issues a special instruction that retrieves the token from the register and provides the token to the hardware. *Id.* 19:43-50. The token that is provided by the user program (retrieved from the register) is compared to a token assigned to a protected page frame,

and if the tokens match, the hardware permits the user program to update the protected memory location. *Id.* 19:59-67.

Significantly, as specifically taught by Bryant, the user program stores the token in the register **for future use**, i.e., for subsequent retrieval when using one of the special instructions. *Id.*, 17:35-37. As further taught by Bryant, "other programs can be authorized to store to the protected page if they are provided with the location of the register storing the token." *Id.* 17:37-40. Thus, Bryant actually would have led a person of ordinary skill in the art **away** from the claimed invention, which recites that the memory protection key in the memory write command that has been written to the volatile memory is rendered **inaccessible** by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory **inaccessible after completion of the memory write command**.

The Response to Arguments section of the Office Action attempts to rebut the foregoing arguments by citing column 5, line 56 – column 6, line 6, of Bryant. Specifically, the Examiner referred to the discussion in Bryant that a user program issues a special instruction that retrieves the **previously stored token from its register**. 5/20/2009 Office Action at 3. According to the Examiner, Bryant "inherently requires storing the token to a volatile memory separate from the aforementioned register for the verification process." *Id.* Retrieving the token from the register to volatile memory does not change the fact the Bryant still teaches the storage of a token in a register for future use, in contradiction of the subject matter of claim 22, which recites rendering the memory protection key in the memory write command that has been written to the volatile memory inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory

protection key in the volatile memory inaccessible after completion of the memory write command. In Bryant, persistent storage of the token is provided such that the goal of rendering the token inaccessible as recited in claim 22 cannot be achieved.

Even assuming for the sake of argument that the Examiner is correct in stating that Bryant would inherently require storing the token of the register in volatile memory, it is noted that there would be absolutely no reason whatsoever to render the memory protection key in the memory write command that has been written to volatile memory inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command, since Bryant specifically teaches that the key would remain accessible for future use in the register. Thus, it would be clear that Bryant would not take the unnecessary step of rendering a version of the key in volatile memory inaccessible, while allowing the key in the register to remain accessible for future use.

The teachings of Bryant relating to token storage for future use would have led a person of ordinary skill in the art **away** from the claimed invention, and **away** from using the techniques mentioned in Bishop regarding erasing, deleting, or deallocating sensitive information. Stated differently, if the techniques of Bishop were to be applied to the teachings of Bryant, then Bryant would have been **rendered inoperable for its intended purpose**, which is to allow the token in the register to be accessible for future memory operations or even for use by other programs. The objective evidence of record thus establishes that a person of ordinary skill in the art would have found no reason to combine the teachings of Bryant and Bishop to achieve the claimed invention.

In view of the foregoing, it is respectfully submitted that the obviousness rejection of claim 22 and its dependent claims is erroneous.

Reversal of the final rejection of the above claims is respectfully requested.

2. Claims 26-28.

Claims 26-28 depend from claim 44, which in turn depends from claim 25, which depends from claim 22. Therefore, claims 26-28 are allowable for at least the same reasons as base claim 22. Moreover, it is respectfully submitted that the rejection of claims 26-28 over Bryant and Bishop is erroneous since the Examiner had **not** rejected intervening claim 44 over Bryant and Bishop. Claim 44 specifically recites receiving, by a wireless receiver, a remote software update to be written to the protected memory location. This feature is clearly not disclosed by or hinted at by Bryant and Bishop.

Therefore, since claims 26-28 depend from claim 44, it is clear that the subject matter of claims 26-28 is not disclosed or hinted at by the hypothetical combination of Bryant and Bishop.

Claims 26-28 are therefore further allowable for the foregoing reasons.

Reversal of the final rejection of the above claims is respectfully requested.

3. Claims 1, 9, 10, 41, 46.

Independent claim 1 is allowable over Bryant and Bishop for similar reasons as those stated above with respect to claim 22. Specifically, claim 1 recites that if a received memory command includes a memory protection key corresponding to each protected memory to be altered, the memory command is permitted to proceed, and the memory protection key in the memory command is then rendered inaccessible by overwriting at least a portion of the memory protection key written to the volatile storage such that the memory protection key written to the volatile storage is inaccessible after completion of the memory command.

As noted above, Bryant would have led away from the claimed invention, and from using the techniques mentioned in Bishop regarding erasing, deleting, or deallocating sensitive information. Specifically, Bryant discloses that a token stored in a register is kept to allow for future access, which is contrary to the subject matter of claim 1.

Since no reason existed that would have prompted a person of ordinary skill in the art to combine the teachings of Bryant and Bishop, the obviousness rejection of claim 1 and its dependent claims over Bryant and Bishop is erroneous.

Reversal of the final rejection of the above claims is respectfully requested.

B. Claims 1, 2, 4, 7-9, 11-15 and 46 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Beukema US Patent Application Publication No. 2002/0124148 in view of Bishop

1. Claims 1, 2, 4, 7-9, 11-15, 46.

The obviousness rejection of claim 1 over Beukema and Bishop is also defective. Beukema describes accessing a protection/translation table to retrieve a protection key, and to compare the protection key to a protection key received in an access to main memory. Beukema, ¶ [0054]. However, there is no hint in Beukema of any desirability to render this protection key inaccessible by overwriting at least a portion of such protection key. Therefore, a person of ordinary skill in the art would not have been prompted to combine the teachings of Beukema and Bishop to achieve the claimed subject matter.

In fact, this point is reinforced by the teachings of Bryant, which constitutes objective evidence that a person of ordinary skill in the art would have been led away from the claimed invention.

In view of the foregoing, it is respectfully submitted that the obviousness rejection of claim 1 and its dependent claims over Beukema and Bishop is erroneous.

Reversal of the final rejection of the above claims is respectfully requested.

C. Claims 16, 17, 19, 20, 22, 25, 36, 39, 43-45 and 47 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hind, US 6,976,163 in view of Bryant and Bishop

1. Claims 16, 17, 19, 20, 36, 39, 43, 45, 47.

Independent claim 16 is non-obvious over Hind, Bryant, and Bishop.

Claim 16 recites an electronic device comprising:

- a memory;
- a wireless receiver configured to receive data relating to a remote software update to be written to the memory;
- a memory protection system associating protected memory locations in the memory with respective corresponding keys, and configured to allow the received data to be written to any of the protected memory locations only if the received data includes a key corresponding to the protected memory location to which the received data is to be written and to render the corresponding key in the received data inaccessible after allowing the received data to be written to the protected memory location; and
- volatile storage having unprotected memory locations, the memory protection system configured to download the received data including the key to the unprotected memory locations of the volatile storage prior to writing the received data to the protected memory locations, and the memory protection system to render the key inaccessible by overwriting at least a portion of the key.

With respect to claim 16, the Examiner stated that "Hind discloses an electronic device comprising a memory; a wireless receiver configured to receive data relating to a remote software update to be written to the memory, and means to securely update the software files via update rules." 5/20/2009 Office Action at 14-15. It is noted that claim 16 does not recite "means to securely update the software files via update rules." In any event, it appears that the Examiner has conceded that Hind fails to disclose all remaining elements of claim 16, including the "memory protection system" element and the "volatile storage" element of claim 16. Instead, the Examiner cited Bryant as purportedly disclosing these claimed features that were conceded to be missing from Hind. *Id.* at 15-16.

The "memory protection" clause of claim 16 recites that the memory protection system is configured to allow the received data to be written to any of the protected memory locations only if the received data includes a key corresponding to the protected memory location to which the received data is to be written and to render the corresponding key in the received data inaccessible after allowing the received data to be written to the protected memory location.

The "volatile storage" clause of claim 16 recites:

> volatile storage having unprotected memory locations, the memory protection system configured to download the received data including the key to the unprotected memory locations of the volatile storage prior to writing the received data to the protected memory locations, **and the memory protection system to render the key inaccessible by overwriting at least a portion of the key**.

As discussed above, Bryant would have led a person of ordinary skill away from the foregoing claimed subject matter, since Bryant contemplates that the token contained in its register is made accessible for **future use** by the user program or by other programs. Bryant, 17:35-40. Thus, a person of ordinary skill in the art would have been led away from making the combination of Hind, Bryant, and Bishop to achieve the subject matter of claim 16. In fact, if the teachings of Bishop were to be incorporated into Bryant, then Bryant would be rendered inoperable for its intended purpose.

In view of the foregoing, it is respectfully submitted that the obviousness rejection of claim 16 and its dependent claims is erroneous. Independent claim 36 and its dependent claims are also similarly allowable over Hind, Bryant, and Bishop.

Reversal of the final rejection of the above claims is respectfully requested.

2. Claims 22, 25, 44.

Independent claim 22 was also rejected as obvious over Hind, Bryant, and Bishop (rather than just over Bryant and Bishop as discussed above).

In the rejection of claim 22, the Examiner cited Hind as purportedly disclosing "a method to remotely update software via update rules contained in the update; receiving the update comprises receiving, via a wireless receiver." 5/20/2009 Office Action at 17. It is noted that claim 22 does not recite the subject matter that was paraphrased on page 17 of the Office Action in the rejection of claim 22. In any event, it appears that the Examiner has conceded that Hind fails to disclose the remaining elements of claim 22. The Examiner cited Bryant and Bishop as purportedly disclosing the vast majority of the elements of claim 22. *Id.* at 18-19.

As discussed above, it is clear that Bryant provides absolutely no hint whatsoever of rendering the memory protection key in the memory write command that has been written to the volatile memory inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory inaccessible after completion of the memory write command. In fact, Bryant would have led away from the claimed subject matter and from a combination with Bishop.

Therefore, a person of ordinary skill in the art clearly would not have been prompted to combine the teachings of Hind, Bryant, and Bishop to achieve the claimed invention. As noted above, if the techniques of Bishop were to be applied to the teachings of Bryant, then Bryant would be rendered inoperable for its intended purpose, which is strongly indicative of the fact that a person of ordinary skill in the art would not have been prompted to combine the teachings

of the references to achieve the claimed invention. Therefore, claim 22 and its dependent claims are also non-obvious over Hind, Bryant, and Bishop.

Reversal of the final rejection of the above claims is respectfully requested.

D. Claims 1 and 3-6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over England, US 7,194,092 in view of Bishop

1. Claims 1, 3-6.

The obviousness rejection of independent claim 1 over England and Bishop is also erroneous.

England refers to an application passing a rights manager certificate and application storage key to a digital rights management operating system (DRMOS). The DRMOS validates the key and compares the rights manager certificate against an access predicate. The DRMOS also determines if the application's use of the content is permitted under the license and allows access if it is. England, 10:41-51. However, England does not disclose or hint at rendering a memory protection key inaccessible by overwriting at least a portion of the memory protection key. In fact, there is nothing in England to hint at any desirability of incorporating such a feature. Therefore, a person of ordinary skill in the art would not have been prompted to incorporate the teachings of Bishop in England to achieve the claimed subject matter.

Again, the teachings of Bryant constitute objective evidence that a person of ordinary skill in the art would have been led away from the invention. Therefore, claim 1 and its dependent claims are also non-obvious over England and Bishop.

Reversal of the final rejection of the above claims is respectfully requested.

CONCLUSION

In view of the foregoing, reversal of all final rejections and allowance of all pending claims is respectfully requested.

Respectfully submitted,

Date: November 2, 2009

/Dan C. Hu/

Dan C. Hu
Registration No. 40,025
TROP, PRUNER & HU, P.C.
1616 South Voss Road, Suite 750
Houston, TX 77057-2631
Telephone: (713) 468-8880
Facsimile: (713) 468-8883

VIII. APPENDIX OF APPEALED CLAIMS

The claims on appeal are (claims 18, 21, 29, 31, 33, 37-38, 40, and 42 have been cancelled):

1. A memory protection system comprising:

a key store to store identifiers of protected memory locations and respective corresponding memory protection keys; and

a memory access manager including at least hardware configured to:

receive a memory command for altering contents of any of the protected memory locations,

determine whether the memory command includes a memory protection key corresponding to at least one of said protected memory locations to be altered, wherein the memory protection key in the memory command is written to a volatile memory,

if the memory command includes the memory protection key corresponding to each protected memory location to be altered, permit the memory command to proceed, and

then render the memory protection key in the memory command inaccessible by overwriting at least a portion of the memory protection key written to the volatile storage such that the memory protection key written to the volatile memory is inaccessible after completion of the memory command.

2. The system of claim 1, wherein the identifiers comprise addresses in a protected memory.

3. The system of claim 1, wherein the identifiers comprise names of protected files in a memory.

4. The system of claim 1, wherein the identifiers identify data entries in a protected memory.

5. The system of claim 1, wherein each of the memory protection keys comprises a modified version of a data sequence.

6. The system of claim 5, wherein the modified version comprises a hash of the data sequence.

7. The system of claim 1, wherein the key store stores a mapping table that maps each identifier to a corresponding memory protection key.

8. The system of claim 7, wherein at least one of the identifiers is mapped to multiple corresponding memory protection keys.

9. The system of claim 1, implemented in an electronic device having a memory, the memory comprising the protected memory locations and unprotected memory locations.

10. The system of claim 9, wherein the memory access manager is further configured to receive memory commands for altering contents of the unprotected memory locations, and to permit the memory commands for altering contents of the unprotected memory locations without checking for any memory protection key.

11. The system of claim 1, wherein the memory access manager is further configured to perform the memory command that includes the memory protection key corresponding to each protected memory location to be altered.

12. The system of claim 1, implemented in an electronic device, wherein the memory command is received by the memory access manager from an originating electronic device component, and wherein the originating electronic device component proceeds with the memory command permitted by the memory access manager.

13. The system of claim 12, wherein the originating electronic device component is a memory update module.

14. The system of claim 12, wherein the originating electronic device component sends memory commands to the memory access manager responsive to data received at the electronic device.

15. The system of claim 14, wherein the originating electronic device component is further configured to extract a received memory protection key from the received data and to provide the received memory protection key to the memory access manager.

16. An electronic device comprising:

a memory;

a wireless receiver configured to receive data relating to a remote software update to be written to the memory;

a memory protection system associating protected memory locations in the memory with respective corresponding keys, and configured to allow the received data to be written to any of the protected memory locations only if the received data includes a key corresponding to the protected memory location to which the received data is to be written and to render the corresponding key in the received data inaccessible after allowing the received data to be written to the protected memory location; and

volatile storage having unprotected memory locations, the memory protection system configured to download the received data including the key to the unprotected memory locations of the volatile storage prior to writing the received data to the protected memory locations, and the memory protection system to render the key inaccessible by overwriting at least a portion of the key.

17. The electronic device of claim 16, wherein the volatile storage is part of the memory.

19. The electronic device of claim 16, wherein the memory protection system comprises:

a key store storing a mapping table that associates the protected memory locations with the respective corresponding keys; and

a memory access manager configured to:

process a memory command for writing the received data to any of the protected memory locations,

determine whether the received data includes the key corresponding to any of the protected memory locations to which the received data is to be written,

if the received data includes the key corresponding to a protected memory location to which the received data is to be written,

permit the memory command to proceed, and

then render the corresponding key in the received data inaccessible.

20. The electronic device of claim 19, wherein the memory comprises a file system, and wherein the key store resides at a secure location in the memory outside the file system.

22. A method of protecting memory in an electronic device, comprising:

receiving a memory command to access a protected memory location;

determining whether the received memory command is a memory read command to read the protected memory location, or a memory write command to alter the protected memory location;

in response to determining that the received memory command is the memory write command:

identifying a memory protection key corresponding to the protected memory location;

determining whether the memory write command includes the memory protection key corresponding to the protected memory location, wherein at least the memory protection key in the memory write command has been written to volatile memory;

permitting completion of the memory write command if the memory write command includes the memory protection key corresponding to the protected memory location; and

rendering the memory protection key in the memory write command that has been written to the volatile memory inaccessible by overwriting at least a portion of the memory protection key in the volatile memory upon completion of the memory write command to make the memory protection key in the volatile memory inaccessible after completion of the memory write command; and

in response to determining that the received memory command is the memory read command, processing the memory read command to read the protected memory location without checking for any memory protection key.

23. The method of claim 22, wherein permitting comprises performing the memory write command.

24. The method of claim 22, wherein receiving comprises receiving the memory command from an originating electronic device component, and wherein permitting comprises allowing the originating electronic device component to perform the memory write command.

25. The method of claim 22, further comprising:
receiving data to be written to the protected memory location; and
generating the memory write command responsive to receiving the data.

26. The method of claim 44, wherein the received data comprises a received key, and wherein generating comprises extracting the received key from the received data and inserting the received key into the memory write command.

27. The method of claim 26, wherein determining comprises comparing the memory protection key corresponding to the protected memory location with the received key in the memory write command.

28. The method of claim 26, wherein determining comprises retrieving a modified version of the memory protection key corresponding to the protected memory location, modifying the received key in the memory write command to generate a modified received key, and comparing the modified received key to the modified version of the memory protection key corresponding to the protected memory location.

30. The method of claim 22, wherein identifying comprises identifying a protected memory location in the memory write command and accessing a mapping table that maps protected memory locations to respective corresponding memory protection keys.

32. The method of claim 22, further comprising:
receiving memory commands to alter unprotected memory locations; and
permitting completion of the memory commands to alter unprotected memory locations without checking for any memory protection keys.

34. The method of claim 22, wherein said identifying step comprises accessing the memory protection key corresponding to the protected memory location in a key store, the method further comprising:

receiving a command to establish a new protected memory location in the memory and a memory protection key corresponding to the new protected memory location;

establishing the new protected memory location in the memory; and

storing the memory protection key in the key store.

35. A computer-readable medium storing instructions for performing the method of claim 22.

36. A method of protecting electronic memory, comprising:

configuring a memory store of an electronic device into at least one protected memory location and a key store operable to store an identifier of each protected memory location and a respective corresponding memory protection key; and

configuring a processor of the electronic device to provide a memory access manager operable to receive memory commands for altering contents of any of the at least one protected memory location, and for at least one memory command, to:

determine whether the at least one memory command includes a memory protection key corresponding to at least one protected memory location to be modified, said at least one memory command including the memory protection key corresponding to at least one said protected memory location to be modified,

permit the at least one memory command to complete, and

then render each corresponding memory protection key in the at least one memory command inaccessible by overwriting at least a portion of the memory protection key upon completion of the at least one memory command, wherein the at least one memory command corresponds to a remote software update received by a wireless receiver for updating the at least one protected memory location to be modified.

39. A computer-readable medium storing instructions for performing the method of claim 36.

41. The system of claim 1, wherein the memory access manager is configured to further receive a memory read command to read content of a particular protected memory location, the memory access manager to allow the memory read command to proceed to read the content of the particular protected memory location without checking for any memory protection key.

43. The electronic device of claim 16, wherein the memory protection system is configured to further:

receive a memory read command to access a particular one of the protected memory locations,

perform reading of the particular protected memory location in response to the memory read command, without checking for any memory protection key.

44. The method of claim 25, wherein receiving the data to be written comprises receiving, by a wireless receiver, a remote software update to be written to the protected memory location.

45. The method of claim 36, wherein configuring the processor further comprises configuring the processor to receive a memory read command to read a particular one of the protected memory locations, and to permit the memory read command to read the particular protected memory location without checking for any memory protection key.

46. The memory protection system of claim 1, wherein the at least a portion of the memory protection key is overwritten upon completion of the memory command.

47. The method of claim 36, wherein the memory protection key in the at least one memory command is written to volatile memory, and wherein the memory protection key in the at least one memory command is rendered inaccessible by overwriting at least the portion of the memory protection key written to the volatile memory such that the memory protection key written to the volatile memory is rendered inaccessible after completion of the at least one memory command.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.